# Cognitive psychology

Cognitive psychology (Association, 2014) involves studying how our brain acquires, perceives, stores, and processes information. As it involves studies related to the workings of the human brain and how it reacts, its study provides valuable insights into why these cyber-attacks are effective and widespread. As criminals exploit cognitive vulnerabilities, human cognition is susceptible to heuristics and biases like trust and familiarity. To exploit the attackers, use emails or messages that appear real and legitimate, offering lucrative things. The messages or emails are usually created to create a sense of urgency and curiosity. When a person receives such a thing, their cognitive process often leads to overlook its consequences and fall into their trap.

# Social Psychology

As humans, psychological studies reveal that people tend to trust more within social networks. Hence, attackers exploit this and send messages and emails by creating fake accounts or accessing their accounts through unfair means. The heavy social media influence and fear of missing out majorly drive people towards these without verifying the authenticity of these messages or emails.

# Behavioural Psychology

They frequently use strategies including deception, social engineering, and authority appeals. According to behavioural psychology, people frequently follow social standards or comply with commands from those they perceive to be in positions of power. In phishing, criminals pretend to be reputable organizations and send those emails and messages from misspelt domains or pretend they work for that reputable organization to trick people into clicking on harmful links or disclosing sensitive information out of a need to conform or comply.

# Why does social engineering work on people?

Social engineering consists of psychological manipulation that makes the user make security mistakes, allowing attackers to access sensitive information. It usually works for multiple reasons, and a few of them are listed below.

* Due to cognitive biases, people trust people from their social circle and authoritative people more easily, leading to phishing attacks as the attackers use them to access sensitive information by creating a fake identity just like them.
* It also exploits the social trust in the personal and professional networks. Attackers act as reliable sources to exploit people's tendency to believe what friends, coworkers, or associates say. Fear of missing out on chances or information might lead people to act without first confirming the integrity of the message.
* They create a false scenario to manipulate a victim, e.g., an emergency with the family, and ask for help and assistance in a very limited time to gain the victim's empathy and cooperation. These types of attacks are quite popular nowadays.

# Why do many people have a hard time securely using passwords?

There are multiple reasons why people have a hard time securely using passwords, and a few of them are listed below.

* Due to cognitive biases, our brain tends to remember familiar and common things more easily, due to which people often keep passwords closely linked to their data, such as date of birth, etc., and choose convenience over security.
* Due to social influence, people tend to take passwords as a casual thing. If people in their social circle don't prioritize using strong passwords, they also tend to follow them, which leads to losing sensitive information.
* Nowadays, due to outnumbered social media platforms, managing and remembering complex passwords for all of them has become a really difficult job, so people keep a single password for all accounts, which leads to security risks.
* People also suffer due to a lack of awareness of having strong passwords.

# Why does PGP fail to be an effective way to secure email?

Pretty Good Privacy is a data and encryption method used in data. Whenever a sender sends data, it gets encrypted with a private key, and the receiver needs that key to access the data. There are multiple reasons PGP fails, and a few of them are listed below.

* One of the major reasons for its failure is behavioural psychology, as PGP is a complex system that may lead to errors, and debugging and managing some keys is also very difficult. Hence, people usually avoid them and opt for using other techniques.
* As it's not adopted on a large scale, the social influence also creates compatibility issues. Most of the social circle didn't adopt it, so it cannot replace weak passwords without its widespread usage.
* It has many cognitive challenges, as the key management encryption and decryption processes are quite complex and usually comprise errors, discouraging adaptation.

# Why is it so easy to spread malware?

The attackers design malware based on Human Psychology, and they are driven by a complex interplay of Human psychology, including behavioural, social and cognitive factors.

Curiosity is one of the major factors that the attackers exploit by designing exciting and sensational content that forces people to click on certain phishing links or drives them to download files out of sheer curiosity. Socially, trust also plays an important role as people generally have a higher trust level for the content shared by friends and family. This can easily lead the malware to propagate into a social circle without knowing it. Social engineering tactics are routinely used to persuade people to act in ways that benefit attackers, such as posing as authorities or making emotional pleas.